SHAW KELLER LLP

John W. Shaw
I.M. Pei Building
1105 North Market Street, 12th Floor
Wilmington, DE 19801
(302) 298-0700
(302) 298-0701 – Direct
jshaw@shawkeller.com

October 28, 2020

BY CM/ECF
The Honorable Leonard P. Stark
J. Caleb Boggs Federal Building
844 N. King Street
Wilmington, DE 19801-3555

Re: *Blix Inc. v. Apple, Inc.*, C.A. No. 19-1869-LPS

Dear Judge Stark,

I write regarding the Federal Circuit's recent decision in *TecSec, Inc. v. Adobe Inc. et al.*, Case No. 19-2192 (Oct. 23, 2020), attached hereto, which affirmed claims 1 and 8 of U.S. Patent No. 5,369,702 were patent eligible. *TecSec* is particularly probative of the issue currently before the court and supports denial of Apple's motion to dismiss.

Claim 1 of TecSec's patent recites:

> 1. A method for providing multi-level multimedia security in a data network, comprising the steps of:
>
> A) accessing an object-oriented key manager;
> B) selecting an object to encrypt;
> C) selecting a label for the object;
> D) selecting an encryption algorithm;
> E) encrypting the object according to the encryption algorithm;
> F) labelling the encrypted object;
> G) reading the object label;
> H) determining access authorization based on the object label; and
> I) decrypting the object if access authorization is granted.

Id. *2-*3. Claim 8 of the TecSec patent is a system claim to "carry out the steps of claim 1's method." *Id.* *4. Appendix A to this letter compares the TecSec and Blix patent claims.

The Federal Circuit affirmed TecSec's claims were patent eligible, emphasizing that Step 1 of the eligibility analysis "depends on an accurate characterization of what the claims require and of what the patent asserts to be the claimed advance." *Id.* *24. It rejected as "materially inaccurate" defendant's assertion that "the claims are directed to the impermissibly abstract idea of managing access to objects using multiple levels of encryption." *Id.* *25. Instead, the claims "go[] beyond managing access to objects using multiple levels of encryption," and "expressly require[] as well, accessing an 'object-oriented key manager' and specified uses of a 'label' as well as encryption for the access management." *Id.* *26. The Federal Circuit cautioned that "[t]o disregard those express claim elements is to proceed at 'a high level of abstraction' that is

'untethered from the claim language' and that 'overgeneralizes the claim." *Id*. *26 (quoting *Enfish*, 882 F.3d at 1337).

The Federal Circuit concluded TecSec's claims were "directed to improving a basic function of a computer data-distribution network, namely, network security." *Id*. *27. Although "non-computer settings may have security issues addressed by multilevel security," the Federal Circuit warned that "*it does not follow that all patents relating to multilevel security are necessarily ineligible for patenting*." *Id*. (emphasis added). Rather, TecSec's claims were eligible because they "improv[ed] a data network used for broadcasting a file to a large audience, with the improvement assertedly being an efficient way for the sender to permit different parts of the audience to see different parts of the file." *Id*. *27-*28; *see also id*. *28 (claims "improv[ed] a data network's basic functioning by enabling secure and efficient transmission to intended recipients when use is made of the basic multicasting functionality of such a data network"). The Federal Circuit also faulted defendant's failure to "meaningfully address the *combination*" of claim element and defendant's focus on the allegedly "commonplace character of the *individual* component techniques generally." *Id*. *30 (emphases added). This "is insufficient" where "the combination of techniques" – not a single element – "is what the patent asserts to be the focus of the claimed advance over the prior art." *Id*. *30.

Apple repeats the same errors as Defendant Adobe in *TecSec*. Apple's proposed abstract idea – "facilitating anonymous communications via a proxy / go-between" (Dkt. 17 at 10) – is, like *TecSec*, "materially inaccurate." *TecSec* at *25. Apple ignores multiple claim limitations that combine to improve electronic communications, including "pre-interaction" utilizing private and public "interaction addresses" and electronic "records" and "reverse lists" associated in a specific manner. (Dkt. 13 ¶ 46-47.) This novel architecture is "directed to improving a basic function of a computer [] network," as in *TecSec* – namely, improving management of anonymous electronic communications. *TecSec* at *27. Here, like *TecSec*, while anonymous communications exist in non-computer settings, "it does not follow that all patents relating to [anonymous communication] are necessarily ineligible for patenting." *Id.* Blix's patent claims a specific architectural improvement for electronic communication, like *TecSec* – a combination the Patent Office specifically found to be eligible under Section 101. (Dkt. 20, Ex. A.) Apple also fails to "meaningfully address the *combination*" of claim elements, just as defendant did in *TecSec* – an approach that "is insufficient" where, as here, a combination is claimed as the advance over the prior art (*e.g.*, by creating the "pre-interaction" method Blix claims as its advance). *TecSec* at *30.

Respectfully submitted,

/s/ John W. Shaw

John W. Shaw (No. 3362)

cc: Clerk of the Court (by CM/ECF)
All counsel of record (by CM/ECF and email)

Appendix A

TecSec patent claim	Blix patent claim
1. A method for providing multi-level multimedia security in a data network, comprising the steps of: A) accessing an object-oriented key manager; B) selecting an object to encrypt; C) selecting a label for the object; D) selecting an encryption algorithm; E) encrypting the object according to the encryption algorithm; F) labelling the encrypted object; G) reading the object label; H) determining access authorization based on the object label; and I) decrypting the object if access authorization is granted.	17. A method of performing controlled pre-interaction, between a first party and at least one second party, said method comprises: (a) providing at least one private interaction address of said first party; (b) defining at least one manageable public interaction address for said first party; (c) forming a record, wherein said manageable public interaction address is associated with said private interaction address for said first party; said method is characterized by: (d) generating a reverse list, wherein an interaction address of said second party is associated at least with said manageable public interaction address of said first party; (e) performing at least one pre-interaction act, said pre-interaction act comprises: (I) accessing said reverse list; (II) identifying said interaction address of said second party in said reverse list; (f) determining that said manageable public interaction address of said first party is associated, at said reverse list, with said interaction address of said second party; wherein said interaction address of said second party is obtainable from a third party or external services provider, wherein said at least one reverse list entry is formed by synchronizing said interaction address of said second party with said manageable public

	interaction address.
8. A system for providing multi-level multimedia security in a data network, comprising: A) digital logic means, the digital logic means comprising: 1) a system memory means for storing data; 2) an encryption algorithm module, comprising logic for converting unencrypted objects into encrypted objects, the encryption algorithm module being electronically connected to the system memory means for accessing data stored in the first system memory; 3) an object labelling subsystem, comprising logic means for limiting object access, subject to label conditions, the object labelling subsystem being electronically connected to the system memory means for accessing data stored in the system memory means and the object labelling subsystem being further electronically connected to the encryption algorithm module to accept inputs from the encryption algorithm module; 4) a decryption algorithm module, comprising logic for converting encrypted objects into unencrypted objects, the decryption algorithm module being electronically connected to the system memory means for accessing data stored in the system memory means; and	27. A system for performing a controlled pre-interaction, between a first party and at least one second party, said system comprises: (a) at least one member selected from the group consisting of: a graphical user interface, input device and computer networking terminal, configured for providing at least one private interaction address of said first party; (b) at least one member selected from the group consisting of: a graphical user interface, input device and computer networking terminal, configured for defining at least one manageable public interaction address for said first party; (c) at least one non-transitory computer storage memory configured for forming and storing a record, wherein said manageable public interaction address is associated with said private interaction address for said first party; (d) at least one computer non-transitory storage memory configured for forming and storing at least one reverse list entry, wherein an interaction address of said second party is associated at least with said manageable public interaction address of said first party; (e) at least one microprocessor configured for accessing said reverse list; (f) at least one microprocessor configured for identifying said interaction address of said second party in said reverse list; and (g) at least one microprocessor configured for determining whether said manageable public interaction

5) an object label identification subsystem, comprising logic for limiting object access, subject to label conditions, the object label identification subsystem being electronically connected to the system memory means for accessing data stored in the system memory means and the object label identification subsystem being further electronically connected to the decryption algorithm module to accept inputs from the decryption algorithm module; B) the encryption algorithm module working in conjunction with the object labelling subsystem to create an encrypted object such that the object label identification subsystem limits access to an encrypted object.	address of said first party is associated, at said reverse list, with said interaction address of said second party; wherein said interaction address of said second party is obtainable from a third party or external services provider, wherein said at least one reverse list entry is formed by synchronizing said interaction address of said second party with said manageable public interaction address.